John Dunbar, OSB #842100
jdunbar@lvklaw.com
Larkins Vacura Kayser LLP
121 SW Morrison St Suite 700
Portland, Oregon 97204
Telephone: 503-222-4424

Richard M. Hagstrom, MN SB 0039445
rhagstrom@hjlawfirm.com
Hellmuth & Johnson, PLLC
8050 West 78th Street
Edina, Minnesota 55439
Tel: (952) 941-4005
Fax: (952) 941-2337

(Additional counsel listed on signature page)

Attorneys for Plaintiff Alliance Healthcare System, Inc. and Proposed Class

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

ALLIANCE HEALTHCARE SYSTEM, INC., on behalf of itself and all others similarly situated, Plaintiff, v. **INTEL CORPORATION,** Defendant.	Case No. **CLASS ACTION ALLEGATION COMPLAINT** (Strict Liability; Negligence; Breach of Warranty; Unfair, Deceptive, and Unlawful Business Practices) **DEMAND FOR JURY TRIAL**

INTRODUCTION

1. Alliance Healthcare System, Inc. ("AHS" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this class action complaint against Defendant Intel Corporation ("Intel" or "Defendant").

2. AHS brings this action to recover substantial damages resulting from incurable security defects in central processing units ("CPUs") designed, manufactured and marketed by Intel that render private medical records and other protected information vulnerable to hacking. AHS makes the following allegations, which are based upon the investigation of counsel, Plaintiff's personal knowledge, and information and belief:

PARTIES

A. Plaintiff

3. Plaintiff Alliance Healthcare System, Inc. is a for-profit health care provider doing business in Holly Springs, Mississippi and incorporated under Delaware law. Plaintiff has purchased servers, personal computers ("PCs") and other devices with Intel CPUs that include the incurable security defects described in this Complaint.

4. Plaintiff's mission is to provide high quality health care that is readily accessible, cost effective and meets the needs of the citizens of the Mississippi communities it serves in and around Holly Springs. To that end, Plaintiff spends substantial sums annually on information technology ("IT") capital and operations.

B. Defendant

5. Defendant Intel is a Delaware corporation with its principal place of business in Santa Clara, California. At all relevant times, Intel was in the business of designing, manufacturing and marketing computer products worldwide, including the defectively designed CPUs at issue.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this controversy pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2)(A), because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of

the Class, and the aggregate amount in controversy for the Class exceeds $5 million exclusive of interest and costs.

7. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over both parties. AHS submits to the Court's jurisdiction. Intel has substantial operations located within this District including manufacturing facilities.

9. Venue is proper under 28 U.S.C. §1391 because many of the acts and transactions underlying this action occurred in this District and because: (a) Defendant is authorized to conduct business in this District and has intentionally availed itself of the laws and markets within this District through the promotion, marketing, distribution, and sale of its defective CPUs; (b) Defendant conducts substantial business in this District; and (c) Defendant is subject to personal jurisdiction in this District.

FACTUAL BACKGROUND

10. As of 2017, Intel was the world's largest manufacturer of semiconductor chips ("CPUs") – the hardware component responsible for interpreting and executing most of the commands from a computer's other hardware and software. The CPU is the brain of a server, personal computer, laptop, or mobile device. Intel sells its CPUs individually and as components of servers, personal computers and mobile devices manufactured by other companies, such as Apple, Asus, Acer, Google, Lenovo, Hewlett Packard, and Dell. It has been reported that 90% of the approximately 1.5 billion personal computers in use today are powered by Intel CPUs. Intel CPUs provide the "brains" of the majority of servers and personal computers, along with those of other devices, utilized in the health care and other industries.

11. Speed and security are two of the most essential features in a CPU, and Intel's success is largely based on the advertised speed and security of its CPUs. But Intel's focus on producing a faster CPU left its CPUs with security vulnerabilities.

12. In 1995, Intel began designing its CPUs to perform a process known as "speculative execution," which increases performance by allowing a CPU to predict its next set of instructions. However, Intel has known or should have known for many months and many years, and admitted publically on January 3, 2018, that speculative execution creates serious security vulnerabilities. These vulnerabilities – dubbed "Meltdown" and "Spectre" –can be exploited by hackers to steal passwords, encryption keys, photos, emails, instant messages, sensitive business documents, and other sensitive data (collectively, "the Defects").

13. These design flaws in Intel's CPUs are the result of Intel's decision to prioritize performance over security.

14. The Defects exist in nearly every Intel CPU manufactured in the last 20 years and, thus, affects most servers, personal computers, laptops, or mobile devices in use today ("Affected Devices").

15. Health care providers such as AHS are obligated by federal law under the Health Insurance Portability and Accountability Act ("HIPAA") and the American Recovery and Reinvestment Act ("ARRA") to protect their patients' medical records and to make those records available to patients in a secure manner via Internet-connected servers. AHS relied upon Intel's representations that its CPUs were secure and fit for use in servers, PCs and other devices that store or access sensitive patient medical records.

16. As a result of the defects disclosed by Intel, and in order to comply with its privacy obligations, AHS has been and will be required to (a) undertake temporary measures to

mitigate the security risks posed by "Meltdown" and "Spectre," which have the side effect of slowing the performance of its computing resources; (b) incur additional costs monitoring its computing resources for security breaches; and (c) replace its computing resources on an accelerated schedule and at significant expense with CPUs that, when available, are not susceptible to these security risks.

17. The enormous costs in responding to the "Meltdown" and "Spectre" security vulnerabilities are being borne by thousands of healthcare and other organizations around the country such as banks, financial institutions, government entities and other entities that, like AHS, are entrusted with sensitive third-party data. Plaintiff brings this action individually and on behalf of a Class of all similarly situated entities in the United States that purchased Affected Devices and are subject to HIPAA or other federal and state laws or regulations imposing standards of care with respect to the protection of third-party information.

a. Federal Law Obligates Health Care Providers to Create, Maintain and Protect Patient Medical Records.

18. AHS and all health care providers are subject to obligations under HIPPA, ARRA, and attendant regulations and other bodies of law, which impose national standards with respect to the secure storage and handling of confidential patient information.

19. HIPAA establishes a national standard that requires health care providers and their business associates to develop and follow procedures ensuring the confidentiality and security of protected health information ("PHI"), including electronic PHI ("ePHI"), when it is transferred, received, handled, or shared.

20. ARRA requires health care providers like Plaintiff to make "meaningful use" of electronic health records ("EHR") to engage patients and family and to maintain privacy and security of patient health information.

21. Plaintiff and other health care providers are subject to fines imposed by the Office of Civil Rights ("OCR") of the United States Department of Health and Human Services ("HHS") for violations of HIPAA. OCR may impose annual fines up to $1.5 million on a health care provider for violations of HIPAA.

b. Intel CPUs Utilized by Health Care Providers and Other Class Members Obligated to Protect Private Information Contain Significant Security Defects Put that Private Information at Risk.

22. Health care providers, like Plaintiff, and other firms subject to heightened privacy standards under federal or state law, routinely utilize Intel CPUs in their servers, PCs and other computing devices to generate, analyze and store ePHI, EHR and similar protected information.

23. Intel dominates the markets for CPUs used in servers and PCs, with shares estimated to be in excess of 90% and 80%, respectively, in 2017. Intel markets its widely-used CPUs as being fit to "prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft."

24. Intel clearly understands the importance of security to health care providers and others subject to HIPAA. Intel's web site, for instance, states: "Protection of personal health information is a critical priority. Intel®-based technologies can support the need for compliance with local regulation of health care information such as the HIPAA privacy and security rule." That same web page warned that "[t]he financial impact from security breaches in the United States averaged more than USD 5.2 million per event in 2011."

25. In June 2017, a team of researchers at Google's Project Zero discovered "serious security flaws" existing in most of Intel's CPUs. Google's researchers publicly announced these security flaws in a January 3, 2018 statement.

26. The security flaws were reportedly discovered simultaneously by multiple research groups working independently from one another, including, but not limited to, researchers from Cyberus Technology and the Graz University of Technology.

27. Researchers have publicly detailed three vulnerabilities: one called "Meltdown" and two referred to as "Spectre." These vulnerabilities are "privilege escalation" flaws, meaning that computer code running in less secure user programs such as web browsers, email clients, and media applications can surreptitiously access the secure kernel or other computer memory to gain access to sensitive data, including user names, passwords, encryption keys and other private data.

28. Upon information and belief, Intel was or should have been aware of the security flaws prior to Google's disclosure. The Defects exist in nearly every Intel CPU manufactured in the last 20 years and, thus, affects most PCs, laptops, smartphones, tablets, and servers in use today.

29. Intel has admitted to having knowledge of the Defects for at least six months, yet during that time, Intel continued to manufacture, sell, and distribute its defective CPUs without disclosure of the Defects. Intel knew or should have known of the Defects long ago but either failed to disclose the Defects or was negligent or reckless in failing to discover them. Indeed, working without the benefit of Intel's proprietary information, at least three security researchers independently discovered the Defects in 2017. With its inside knowledge and familiarity with the design and inner workings of its CPUs, Intel was in a better position to discover the Defects than third-party researchers and, as the manufacturer of the defective CPUs that it introduced into the market, Intel had a duty to do so.

///

c. Intel's Modern Central Processing Units

30. User programs are made up of CPU instructions that are ordered to be processed and executed serially, one after the other, akin to water moving through a single pipeline. Intel's CPUs contain more than one "pipeline" for ordering and executing a user program's instructions. A single-pipeline CPU would take eight cycles to process eight instructions; a CPU with eight pipelines could, under ideal circumstances, process those same eight instructions in one cycle.

31. In order to take advantage of multiple pipelines, Intel's CPUs make "guesses" as to what CPU instructions may be executed after any particular instruction via a process known as "branch prediction." Branch prediction utilizes algorithms to determine what instructions are most likely to be executed after another instruction (the "prime instruction"), gathers the predicted instructions and data inputs from memory, and speculatively executes those instructions in anticipation of providing the results after execution of the prime instruction, with the entire process known as "speculative execution."

32. While Intel's implementation of branch prediction and speculative execution in its CPUs has greatly increased the performance of those processors, its particular design decisions have introduced grave security flaws.

d. "Spectre"

33. The "Spectre" security flaws are integral to the design of Intel CPUs and utilize speculative execution of privileged code: A malicious program trains the CPU to predict that otherwise protected memory will be relevant to a future operation and the CPU is fooled into making that protected memory available to the malicious program.

34. In the context of PCs, malicious programs such as pretextual advertisements in web browsers can be used to obtain usernames and passwords that provide access to sensitive,

valuable, and confidential data, including patient records, financial information, and client files. In addition to being attacked via web advertising, computers are susceptible to these attacks via email, instant messaging, and malware.

35. The "Spectre" threat to cloud-based servers is particularly extreme. Cloud-based virtual server hosting is increasingly common with vendors such as Microsoft, Amazon, IBM, Salesforce.com, SAP, Oracle, Google, ServiceNow, Workday, VMware, and others providing shared server resources directly and indirectly to consumers like Plaintiff AHS. In this circumstance, vendors utilize a number of physical Intel CPUs to provide many times that number of virtual CPUs to cloud customers.

36. A malicious actor could exploit Intel's "Spectre" design flaws by, for example, purchasing a virtual server in the cloud and running a program that permits access to other virtual servers running on the same Intel CPU. Such a malicious server sharing space with servers for hospitals, banks, and law firms could gain complete access to the memory of those virtual servers and, consequently, gain complete access to all of those servers' sensitive data.

e. <u>"Meltdown"</u>

37. "Meltdown" is a hardware vulnerability that tricks the CPU into speculatively loading data that has been marked unreadable or "privileged." This flaw potentially allows malicious programs to request protected kernel memory and to access copies of the protected memory.

38. Metadata associated with operating system memory determines whether it can be accessed by user programs or is restricted to the kernel. Intel CPUs allow programs to speculatively use kernel data, with the access check (which verifies whether the kernel memory is accessible to a user program) occurring only sometime after the instruction starts executing.

While speculative execution is blocked when the check occurs, the impact that speculation has on the CPUs cache can be used to infer the values stored in kernel memory.

39. As a result of the "Meltdown" vulnerability, Intel's CPUs are potentially susceptible to JavaScript exploits that allow attackers to obtain sensitive web browser information, including cookies, credentials, passwords, or payment information that a user has entered into a browser. In the case of Plaintiff and other Class members, that browser data could also include PHI or other protected third-party information.

f. "Meltdown" and "Spectre" Cannot be Fixed in Existing CPUs.

40. While the security risks associated with "Meltdown" and "Spectre" can be mitigated, only a full redesign of Intel's CPUs can remedy these defects and eliminate the security vulnerabilities.

41. Intel's first January 2018 statement downplayed the seriousness of the vulnerabilities and disputed reports that software and firmware patches to mitigate those threats would impact the performance of a CPU. However, days later, Microsoft issued a statement addressing the Meltdown and Spectre vulnerabilities and confirmed that software mitigation patches will result in slowdowns on many PCs and all servers.

42. Software patches have been issued for various operating systems (including Microsoft's Windows, Apple's macOS, and Linux) to mitigate against "Meltdown" and "Spectre."

43. In some instances, software running on Intel CPUs and microcode running within Intel CPUs can be modified to reduce, but not eliminate, the risk. However, when available, these techniques reduce the performance of the CPUs, particularly for CPU operations involving

numerous input/output operations. It has been widely reported that mitigation patches reduce the performance of Intel CPUs by up to 30% or more.

44. In other instances, no mitigation technique is available, and the Intel CPU is inherently insecure.

g. Intel's CPU Security Defects Have Damaged and Will Continually Damage Health Care Providers and Other Entities Subject to Privacy Obligations.

45. Shortly after the "Meltdown" and "Spectre" flaws were disclosed publicly, OCR reportedly sent an email update that urged HIPAA-covered entities to mitigate the vulnerabilities as part of their risk management processes. Given the nature of the CPU flaws, failure to mitigate places at risk the confidentiality, integrity, and availability of PHI.

46. On January 12, 2018, HHS's Health Care Cybersecurity and Communications Integration Center ("HCCIC") issued a technical report on the "Meltdown" and "Spectre" vulnerabilities, which noted "[m]ajor concerns" for the health care sector. These included, but were not limited to:

- Challenges identifying vulnerable medical devices and accessory medical equipment and ensuring patches are validated to prevent impacts to the intended use.
- Cloud Computing: Potential PHI or Personally Identifiable Information (PII) data leakage in shared computing environments.
- Web browsers: Possible PHI/PII data leakage.
- Patches: Potential for service degradation and/or interruption from patches.

47. Plaintiff and other Class members have incurred and will continue to incur costs to monitor protected information, including patient ePHI and EHR, for data breaches and other malicious activity. These monitoring costs are above and beyond the costs that would be incurred as part of their ordinary risk management processes. These additional monitoring costs will

continue until such time as Plaintiff and Class members purchase new CPUs that are not subject to the security risks described above.

48. Additionally, Plaintiff and Class members have been required to expend resources to monitor the efficacy of, and mitigate any adverse effects from, Intel's "patches." These fixes, supposedly designed to mitigate Intel's security defects, have already proven defective, and have caused substantial reliability issues in affected PCs and servers.

49. As the risks posed by "Meltdown" and "Spectre" to protected information become better understood, Plaintiff and other Class members will be required to engage in additional, costly mitigation techniques, including devoting increased labor to the heightened monitoring of their Intel-based systems for security breaches, the procurement and installation of software designed to avoid Intel's CPU defects, and procurement of additional computer hardware to compensate for the reduced performance of mitigated but still dangerously insecure Intel CPUs.

50. Intel has announced that future generations of its CPUs will not contain these defects. If and when Intel corrects its design defects and begins manufacturing and selling CPUs without the flaws described above, Plaintiff and other Class members will be compelled to either purchase a new, non-affected CPU or continue to use defective CPUs with serious security vulnerabilities and/or significantly reduced performance. Consequently, Plaintiff and other Class members will sustain additional damages by expending the costs necessary to upgrade to non-defective computers and servers.

CLASS ACTION ALLEGATIONS

51. Plaintiff brings this action on behalf of itself and as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure seeking damages on behalf of itself and Class Members nationwide (the "Class"):

> All persons or entities in the United States that are subject to federal or state laws or regulations imposing standards of care with respect to the protection of confidential third-party information who, between 1995 and the present, purchased (a) one or more Intel CPU from Intel or its authorized resellers, or (b) one or more servers, PCs or any other device containing an Intel CPU, that are vulnerable to Spectre or Meltdown.

52. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint.

53. Specifically excluded from the Class are Intel, including any of its subsidiaries, joint ventures, or affiliates, any entity in which Intel has a controlling interest; any person who is an officer or director of the aforementioned entities; and the judge assigned to this action, the judicial staff, and any member of the judge's immediate family.

54. Numerosity: While Plaintiff does not know the exact number of the members of the Class, Plaintiff believes there are thousands of entities, and as such, individual joinder is impracticable.

55. Predominance of common questions of law and fact: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. Such questions of law and fact common to the Class include, but are not limited to:

- Whether Intel's CPUs were or are defectively designed;
- Whether Intel's CPUs are affected by the "Meltdown" and "Spectre" flaws;
- Whether the "Meltdown" and "Spectre" flaws put at risk private third-party information entrusted to Class members;
- Whether efforts by Class members to monitor their computing resources and take other steps to mitigate the risks caused by the "Meltdown" and "Spectre" flaws are reasonable;

- Whether Defendant made any express warranties in connection with the sale of its defective CPUs;
- Whether Defendant breached any express warranties in connection with the sale of its defective CPUs;
- Whether Intel made any implied warranties or other representations in connection with the sale or marketing of its vulnerable CPUs;
- Whether Intel breached any duties owed to Class members;
- Whether Defendant's acts and practices violated the "unlawful" prong of the Unfair Competition Law, California Business and Professions Code §§17200, et seq. ("UCL");
- Whether Defendant's acts and practices violated the "unfair" prong of the UCL;
- Whether Defendant's acts and practices violated the "fraudulent" prong of the UCL;
- Whether Defendant was unjustly enriched;
- Whether Plaintiffs and the other Class members have sustained monetary loss and the proper measure of that loss; and
- Whether Plaintiffs and the other Class members are entitled to declaratory and injunctive relief.

56. Typicality: Plaintiff's claims are typical of the claims of the other class members in that the injuries suffered by AHS and the Class arise from the same nucleus of operative facts based on Intel's common course of conduct giving rise to the claims of the other members of the Class. Plaintiff has no interests that are antagonistic to those of the other members of the Class.

57. Adequacy of Representation: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation, including matters involving high-tech markets. Plaintiff's

counsel have worked with renowned technical and industry experts who have significant experience with security flaws.

58. Superiority: Class action treatment is a superior method for the fair and efficient adjudication of the controversy, in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

59. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class members' claims compared to the anticipated costs of the litigation, it is likely that only a few Class members could afford to seek legal redress for the harms caused by Intel's design defects.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Strict Liability

60. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

61. Plaintiff and Class members were harmed by the CPUs Intel manufactured and marketed, which were contained in, but also separate and apart from, the servers, PCs and other devices purchased.

62. Intel's CPUs contained manufacturing defects, or were defectively designed, for the reasons set forth above. As a result, Plaintiff and Class members now own servers, PCs and other devices with Intel CPUs that put at risk the confidential and protected third-party information and other sensitive data on their networks.

63. As a direct result of the manufacturing or design defects, Plaintiff and Class members have been harmed by having to incur mitigation and monitoring costs, in an amount to be determined at trial, and will continue to incur those expenses until their servers, PCs and other devices with defective Intel CPUs can be replaced with hardware that does not suffer from the defects.

64. Moreover, Plaintiff and Class members have been harmed because they are compelled by their duty to protect against privacy breaches to expedite their purchases of next-generation CPUs prior to the expiration of the reasonably expected operating life of the defective CPUs.

SECOND CLAIM FOR RELIEF

Negligence

65. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

66. Intel was negligent in the manufacture and design of the CPUs containing the defects described above, which were contained in, but also separate and apart from, the servers, PCs and other devices that Plaintiff and Class members purchased.

67. Intel's negligence was a substantial factor and reasonably foreseeable in causing harm to Plaintiff and Class members.

68. Plaintiff and Class members have been harmed, as they now own servers, PCs and other devices with CPUs that, due to the manufacturing or design defects described above, put at risk confidential and protected third-party information and other sensitive data on their networks. Plaintiff and Class members are thereby required to incur mitigation and monitoring costs in an amount to be determined at trial, and will continue to have to do so until their servers, PCs and other devices with defective Intel CPUs can be replaced with hardware that does not suffer from the defects.

THIRD CLAIM FOR RELIEF

Breach of Express Warranty

69. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

70. Intel designed, manufactured, advertised, and distributed defective CPUs. Intel is a "merchant" and the Intel CPUs are "goods" within the meaning of the Uniform Commercial Code.

71. In connection with each sale, Intel represented that its CPUs provided a particular level of security, which they did not, and were of particular speeds, which, after implementation of a software patch necessary to mitigate security threats caused by the design defects, they are not.

72. Intel's affirmations of fact and promises relating to its defective CPUs became part of the basis of the bargain and created an express warranty that the CPUs would conform to Intel's affirmations and promises.

73. Intel's express warranties run to Plaintiffs and the other members of the Class either directly or as third-party beneficiaries.

74. Intel breached its express warranties by delivering CPUs that failed to conform to Intel's affirmations and promises.

75. Intel's breach of express warranties directly and proximately caused damages, injury in fact, and ascertainable loss to Plaintiffs and the other members of the Class, in an amount to be determined at trial.

76. All conditions precedent to this claim have been satisfied.

FOURTH CLAIM FOR RELIEF

Breach of Implied Warranties of Merchantability and Fitness for Particular Purpose

77. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

78. Intel, as the designer, manufacturer, marketer, distributor, and/or seller of the defective CPUs at issue, is a merchant with respect to the defective CPUs.

79. As such, a warranty that each CPU was merchantable and fit for a particular purpose was implied in the contract of each sale to Plaintiffs and the other members of the Class.

80. Intel breached the implied warranty of merchantability because:

a. the defective Intel CPUs could not pass without objection in the trade because they are missing a key promoted characteristic, namely not exposing users to critical security vulnerabilities;

b. the CPUs were not of fair average quality;

c. were not adequately advertised, packaged, and/or labeled as omitting material facts as to the presence of the defects; or

d. they did not conform to the promises or affirmations of fact made by Intel.

81. Plaintiff and Class members did not receive goods as impliedly warranted by Intel to be "merchantable." Moreover, as these were latent defects that existed at the time of purchase for the reasons described above, the CPUs are rendered unmerchantable.

82. Intel had reason to know that Plaintiff and Class members were relying on its skill and judgment to furnish suitable goods that would satisfy their particular purposes. Intel had reason to know of the particular purpose of these purchases, and that purchasers would be relying on their skill and judgment to ensure these computers would perform adequately and not subject them to critical security vulnerabilities.

83. The CPUs were not altered by Plaintiff or Class members.

84. The CPUs did not conform to these implied warranties when they left the exclusive control of Intel.

85. Plaintiff and Class members did not receive these goods as impliedly warranted.

86. All conditions precedent to seeking liability for breach of these implied warranties have been performed by or on behalf of Plaintiff and Class members. Intel has refused to recall, repair or replace, free of charge, all Intel CPUs or refund the prices paid for the CPUs.

87. As a direct and proximate cause of Intel's breaches of implied warranties, Plaintiff and Class members have been injured and harmed, in an amount to be determined at trial.

FIFTH CLAIM FOR RELIEF

Violation of Cal. Bus. & Prof. Code § 17200, et seq.: "Unfair" Business Practices

88. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

89. Plaintiff has standing to pursue this claim as AHS has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

90. As alleged herein, Intel engaged in "unfair" business acts and practices by:

a. designing, marketing, distributing, and selling defective CPUs without disclosing that the CPUs contained design defects;

b. refusing to repair or recall the defective CPUs; and

c. refusing or failing to compensate injured consumers, including Plaintiffs and the other members of the Class.

91. Intel's fraudulent business acts and practices in violation of the UCL were likely to deceive, and did in fact deceive, members of the public, including Plaintiffs and the other members of the Class, who suffered injury in fact and lost money or property as the result of Intel's fraudulent business practices.

92. Intel's business practices, including but not limited to its affirmative acts and material omissions, are contrary to public and legislative policy and the harm it has, and continues to cause, Plaintiff and members of the Class far outweighs its utility.

93. As a result of Intel's "unfair" business practices, Plaintiff and members of the Class spent money on servers, PCs and other computing devices that contain Intel's defective CPUs.

94. Intel's unfair business practices constitute a continuing course of unfair competition.

95. Plaintiff and Class members seek an order for injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies wrongfully obtained from Plaintiff and Class members, and all other relief permitted under Bus. & Prof. Code § 17200, *et seq*.

SIXTH CLAIM FOR RELIEF

Violation of Cal. Bus. & Prof. Code § 17200, et seq.:
"Deceptive" Business Practices

96. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

97. Plaintiff has standing to pursue this claim as AHS has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

98. Intel's business practices were "deceptive" because they were and are likely to deceive consumers, including Plaintiff and Class members, targeted by such omissions of material fact. Among other things, Intel failed to disclose material information to purchasers of servers, PCs and other computing devices containing Intel CPUs by concealing material facts relating to critical security vulnerabilities.

99. As a result of Intel's "deceptive" conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

100. Intel's deceptive business practices alleged herein constitutes a continuing course of unfair competition.

101. Plaintiff and the Class seek an order for injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies that have been wrongfully obtained from Plaintiff and the Class, and all other relief permitted under Bus. & Prof. Code § 17200, *et seq*.

///

///

///

///

SEVENTH CLAIM FOR RELIEF

Violation of Cal. Bus. & Prof. Code § 17200, et seq.:
"Unlawful" Business Practices

102. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

103. Plaintiff has standing to pursue this claim as AHS has suffered injury-in-fact and lost money or property as a result of the critical security vulnerabilities in Intel's CPUs.

104. Intel's business practices, including but not limited to its continued marketing of its defective CPUs after learning of the "Meltdown" and "Spectre" vulnerabilities, constitute "unlawful" business practices because they violated California Civil Code § 1750, *et seq*., California Civil Code § 1790, *et seq*., 15 U.S.C. § 2301, et seq., among other laws, breached applicable warranties, and engaged in acts resulting in negligence and strict liability.

105. As a result of Intel's "unlawful" conduct, Plaintiff and Class members spent money on servers, PCs and other computing devices with defective CPUs.

106. Intel's unlawful business practices alleged herein constituted a continuing course of unfair competition.

107. Plaintiff and the Class seek an order for public injunctive relief to benefit the public, including a corrective advertising campaign, requiring Intel to make full disgorgement and restitution of all monies wrongfully obtained from Plaintiffs and the Class, and all other relief permitted under Bus. & Prof. Code § 17200, *et seq*.

EIGHTH CLAIM FOR RELIEF

Unjust Enrichment

108. Plaintiff, individually and on behalf of the Class, incorporate by reference all of the allegations contained in paragraphs 1 through 59 of this Complaint.

109. This cause of action is pled in the alternative.

110. Plaintiffs and the other members of the Class purchased from Defendant and its authorized retailers and resellers defective CPUs they would not otherwise have purchased but for Defendant's failure to disclose the Defects described above.

111. As such, Defendant has been unjustly enriched at the expense of Plaintiffs and the other members of the Class.

112. Under the circumstances, it would be unfair, improper, and unjust for Defendant to retain this financial benefit.

113. Plaintiffs and the other members of the Class have no adequate remedy at law.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all others similarly situated, requests the Court to enter judgment against Intel, as follows:

A. Certifying the proposed Class, designating Plaintiff as the named representative of the Class, and appointing the undersigned as Class Counsel;

B. Awarding Plaintiff and the Class damages, including but not limited to compensatory, statutory and punitive damages, in an amount to be determined at trial;

C. Awarding declaratory, injunctive, and other equitable relief as permitted by law or equity, including enjoining Defendant from continuing the unlawful practices described herein, and directing Defendant to identify, with this Court's supervision, victims of its conduct and to pay them restitution of all monies acquired through any act or practice declared by this Court to be wrongful or unlawful;

D. Awarding restitution and disgorgement of Defendant's revenues to Plaintiffs and the Class;

E. Awarding Plaintiff's reasonable attorneys' fees and costs;

F. Awarding pre-judgment and post-judgment interest, as provided by law; and

G. Awarding such other legal or equitable relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b) and the Local Rules of this Court, Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: April 27, 2018.

LARKINS VACURA KAYSER LLP

s/ John Dunbar
John Dunbar, OSB #842100
jdunbar@lvklaw.com
Larkins Vacura Kayser LLP
121 SW Morrison St Suite 700
Portland, Oregon 97204
Telephone: 503-222-4424

To be Admitted Pro Hac Vice:
Richard M. Hagstrom, MN Bar No. 0039445
rhagstrom@hjlawfirm.com
Michael R. Cashman, MN Bar No. 0206945
mcashman@hjlawfirm.com
Michael P. Srodoski , MN Bar No. 0398250
msrodoski@hjlawfirm.com
8050 West 78th Street
Edina, Minnesota 55439
Tel: 952-941-4005
Fax: 952-941-2337

Quentin Whitwell, MS Bar No. 10859
quentin@harperwhitwell.com
Harper Whitwell, PLLC
800 College Hill Road, Suite 5201
P.O. Box 3150
Oxford, Mississippi 38655
Tel: 662-234-0320
Fax: 662-259-8464

Attorneys for Plaintiff Alliance Healthcare System, Inc. and Proposed Class